

CYBER SECURITY DIVISION  
2013 PRINCIPAL INVESTIGATORS'

**From Local to Global  
Awareness: A Distributed  
Incident Management System  
(DIMS)**

University of Washington  
David Dittrich

*September 17, 2013*

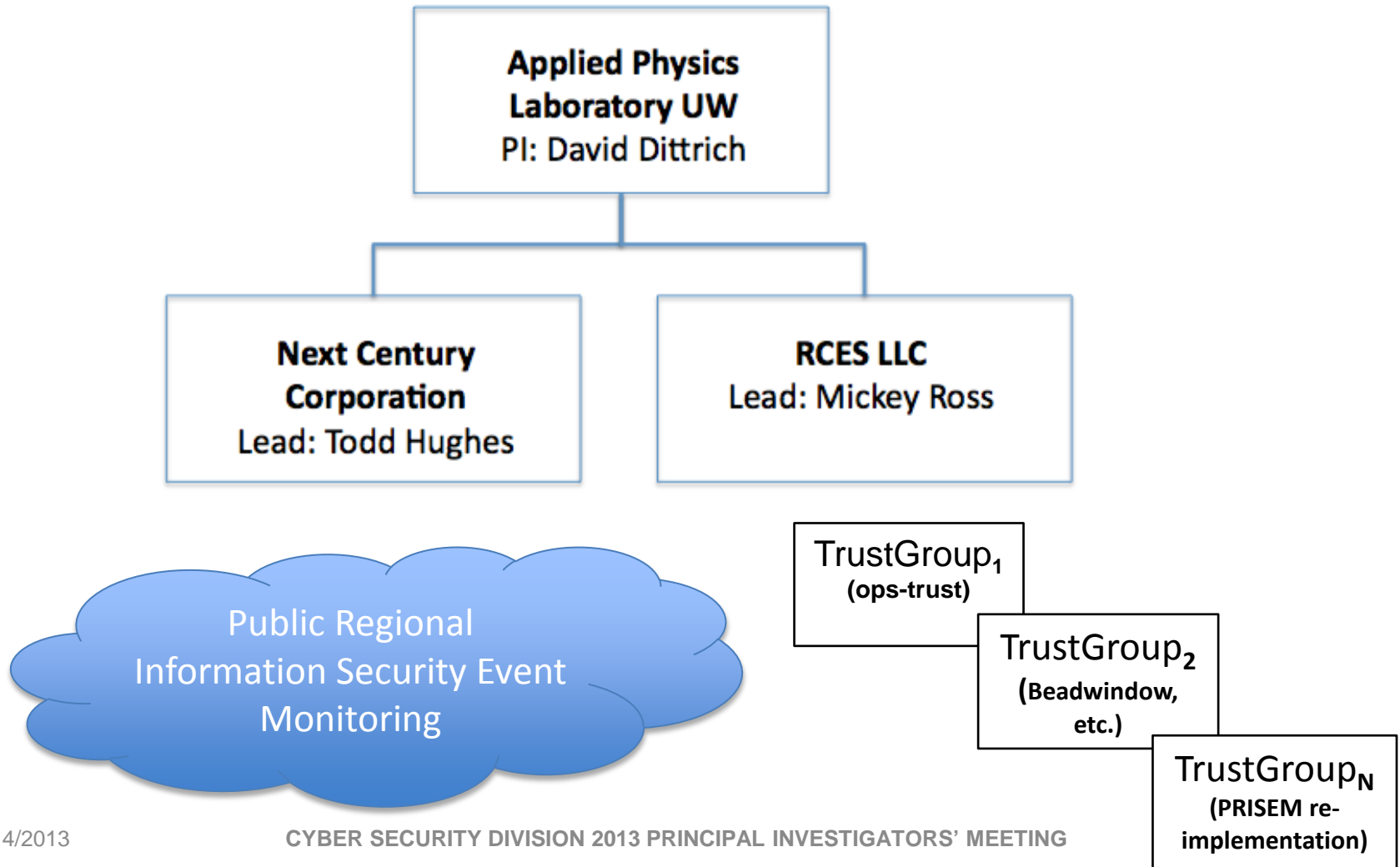


**Homeland  
Security**

Science and Technology



# Team Profile



# Customer Need

**OPERATIONS SECURITY TRUST**

**Mission**

OPSEC-Trust (or "ops-trust") forum is a highly vetted community of security professionals focused on the operational robustness, integrity, and security of the internet. The community provides responsible action against malicious behavior beyond just observation, analysis and research. OPSEC-Trust carefully expands membership pulling talent from many other security forums looking for strong voting in three areas:

1. sphere of trust.
2. sphere of action.
3. the ability to maintain a "need to know" confidentiality.

OPSEC-Trust (or "ops-trust") members are in a position to directly affect internet security operations in some meaningful way. The community's members span the breadth of the industry including service providers, equipment vendors, financial institutions, mail admins, DNS admins, DNS registrars, content hosting providers, law enforcement organizations/agencies, CERT teams, and third party organizations that provide security-related services for public benefit (e.g. monitoring or flagging service providers). The breadth of membership, along with an action plus just vetting approach creates a community which would be in a position to apply focused attention on the malicious behaviors which threaten the internet.

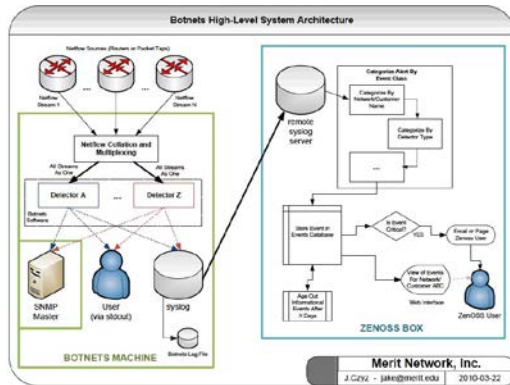
**Members:**

- will be privy to lists of infected IP addresses, compromised accounts, bot c&c lists and other data that should be acted upon.
- are expected to take appropriate action within their domain of control.
- are expected to contribute data as appropriate and in a fashion that does not violate any laws or corporate policies.

OPSEC-Trust does not accept applications for membership. New candidates are nominated by their peers who are actively working with them on improving the operational robustness, integrity, and security of the internet.

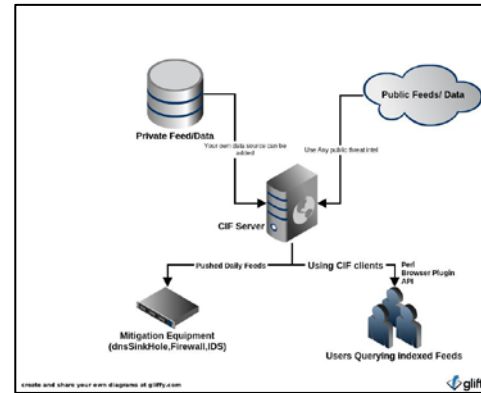
© OpSecTrust

<http://ops-trust.net>

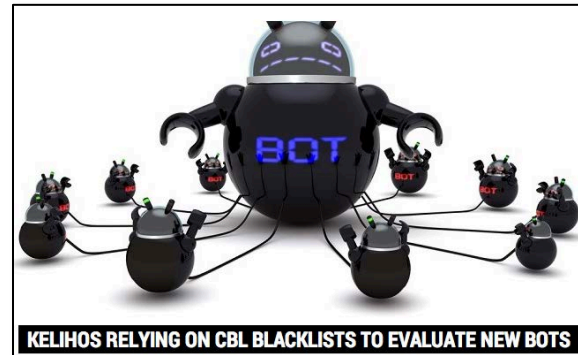


<http://botnets.org>

*Indicators from multiple sources (e.g. Alienvault, Shadowserver, Malwarebytes, Mandiant, etc.)*

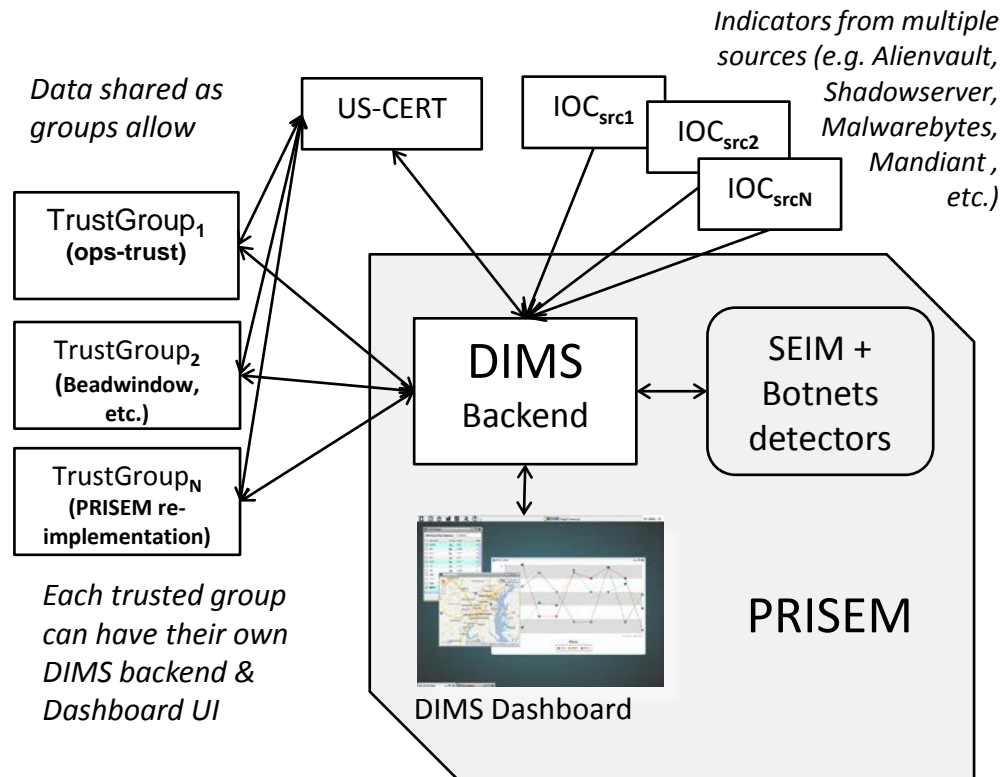


<http://code.google.com/p/collective-intelligence-framework/>



<http://threatpost.com/kelihos-relying-on-cbl-blacklists-to-evalute-new-bots>

# Customer Need



# Approach

*Develop a system for collaborative response detection and mitigation mechanisms to counter target and advanced threats*

- Web Application Service front end (dashboard) for data mining, analysis, reporting, and data ingest/export
- Role based access controls, account management, and data anonymization/filtering
- Integrate alerting from protective and detective systems with contextual information and cross-organizational situational awareness
- Integration with host-based forensic tools to facilitate triage, implementing “course of action” steps
- Vertical (US-CERT) and horizontal information sharing with trusted groups (e.g., ops-trust, Beadwindow, etc.)

# Benefits

- **Improved Performance**
  - Platform for collaborative situational awareness and response, integrating Indicators of Compromise (IOCs) from multiple sources
  - Security-assessed ops-trust portal for increased collaboration across trust groups
  - Improve operator effectiveness in mitigating targeted and advanced threats
  - Provide actionable intelligence and course of action options
- **Lower Cost of Ownership**
  - Prototypes developed as open source for rapid innovation & diffusion
  - Use combined strength of UW, Next Century, to support technology transfer
- **Better situational awareness (at scale)**
  - Integrated approach to monitoring, analysis, visualization, and data sharing
  - Enhance existing Security Event Information Management (SEIM) systems with vendor-neutral dashboard



# Contact Information



- David Dittrich (Principal Investigator)  
dittrich *at* uw *dot* edu  
<http://staff.washington.edu/dittrich/>